

RECEIVED
CENTRAL FAX CENTER

FEB 27 2007

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

REMARKS

Applicants thank the Examiner for the careful and thorough examination of the present application, and for withdrawing several of the previous rejections.

Applicants have amended independent Claims 21 and 31 to address the Examiner's 35 U.S.C. §101 rejection and 35 U.S.C. §112, 1st paragraph rejection. Claims 27-29 have been amended, and Claim 26 has been canceled for consistency. Claims 44-47 have also been canceled for consistency. Applicants also added new independent Claim 48, which includes the subject matter of Claims 21-23 in a different combination.

Applicants submit that all claims are patentable for the reasons presented in detail below.

I. The Claimed Invention

Amended independent Claim 31, for example, is directed to a device for converting data between an unencrypted format and an encrypted format. The device comprises a register for storing the data in the form of bit words, and a circuit. Claim 31 has been amended to recite the circuit is for converting the data, and support for this amendment is found on page 6, lines 23-31 of the present application. Claim 31 further recites that the converting comprises performing a plurality of transformation rounds, with each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array. Furthermore, each of the rows may be exchanged with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that at least one

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

transformation is applied to the transposed state array.
Claim 31 has also been amended to recite applying at least one round key to the state array in at least one of the transformation rounds.

The converting device may provide for increased encryption and decryption speed versus the prior art. (Page 10, lines 27-33). Moreover, this may be achieved while maintaining compliance with the Advanced Encryption Standard (AES), for example. The converting device may permit 32-bit processing.

Amended independent Claim 21 is a method counterpart to Claim 31 and has been similarly amended. New independent claim 48 is similar to Claim 21, but further recites using 8-bit words, and operating on a state array comprising a 4x4 matrix of 8-bit words.

II. The Claims Comply With 35 U.S.C. §112, First Paragraph

The Examiner rejected Claims 21-25 and 31-43 under 35 U.S.C. §112, 1st paragraph, contending that the claimed invention is missing a critical or essential step. The Examiner also contended that applying a key is a critical or essential step to using the Rijndael encryption algorithm, citing the Abstract and the specification of the present application.

Applicants continue to disagree with the Examiner, but in order to advance prosecution, Applicants have amended independent Claims 21 and 31 to recite applying at least one round key to the state array in at least one of the transformation rounds. New independent Claim 48 also includes this recitation to advance prosecution.

In re Patent Application of
MACCHETTI ET AL.

Serial No. 09/974,705

Filed: OCTOBER 10, 2001

III. The Claims Are Patentable

A. The Claims Are Directed To Statutory Subject Matter

The Examiner rejected Claims 21-47 over 35 U.S.C. §101, contending the claims recited only mathematical formula and number calculations. Applicants have amended independent Claims 21 and 31 to recite converting the data. New independent Claim 48 also includes this recitation to advance prosecution. The converting includes performing a plurality of transformation rounds, etc., as recited in the respective independent Claims.

Accordingly, amended independent Claims 21 and 31 are directed towards statutory subject matter. Their respective dependent claims, which recite yet further distinguishing features, are also directed toward statutory subject matter and require no further discussion herein.

B. The Rejection Over Ohkuma Et Al. In View Of Luther Is Overcome

The Examiner rejected independent Claims 21 and 31 over Ohkuma et al. in view of Luther. Ohkuma et al. discloses an apparatus for encrypting blocks of data. (Paragraphs 10-11). The encryption process occurs in multiple stages. (Paragraph 91-92). Ohkuma et al. also discloses that a matrix may be obtained by substituting rows, substituting columns, and arbitrarily transposing an arbitrary MDS matrix. (Paragraph 268). The Examiner correctly notes that Ohkuma et al. fails to disclose exchanging each of the rows with a respective column of the state array to form a transposed state array, as recited in independent Claims 21 and 31. The Examiner looks to Luther to supply such deficiency.

In re Patent Application of
MACCHETTI ET AL.

Serial No. 09/974,705

Filed: OCTOBER 10, 2001

Luther discloses an encryption system for two-dimensional data. The system of Luther encrypts through multiple encryption passes performed on binary data. In each pass, the mth row and the nth column of the binary data are encrypted. For each encryption pass, m and n are randomly selected and have a value which is small relative to the size of the data. (Col. 1, lines 30-42).

The Examiner cites Column 6, lines 12-16 of Luther as disclosing exchanging each of the rows with a respective column of the state array to form a transposed state array, as in the claimed invention. Applicants respectfully disagree with this contention. The cited portion of Luther recites "[w]hen executing steps S211 and S215 for complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column or a shift row/column end around function could be implemented to further confuse the data." Applicants submit that Luther does not supply for the noted deficiency of Ohkuma et al. Indeed, at best, it appears that Luther discloses the same deficient teaching, i.e. arbitrary swapping of the rows and columns of the matrix and not exchanging each of the rows with a respective column as claimed.

Accordingly, amended independent Claims 21 and 31 are patentable. New independent Claim 48 includes similar recitations and is patentable for similar reasons.

Accordingly, it is submitted that amended independent Claims 21 and 31, and new independent Claim 48 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

also patentable over the prior art and require no further
discussion herein.

RECEIVED
CENTRAL FAX CENTER

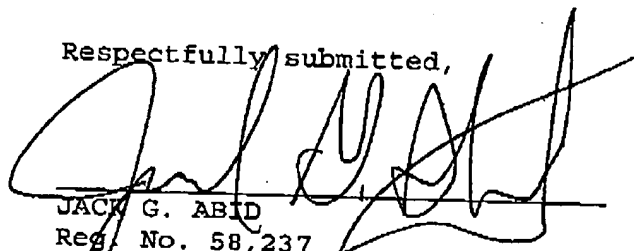
FEB 27 2007

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

CONCLUSIONS

In view of the amendments to the claims and the arguments presented above, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned at the telephone number listed below.

Respectfully submitted,



JACK G. ABID
Reg. No. 58,237
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants

CERTIFICATE OF FACSIMILE TRANSMISSION

I HEREBY CERTIFY that the foregoing correspondence has been forwarded via facsimile number 571-273-8300 to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 this 27th day of February, 2007.

